**Amendment to the Claims:**

This listing of claims will replace all prior versions and listings of claims in the application.

**Listing of Claims:**

1. (Previously Presented) A method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing, by the first digital certificate issuing authority, the electronic document to obtain a once signed electronic document;

transmitting the once signed electronic document to a second digital certificate issuing authority;

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party;

wherein the second digital certificate issuing authority is hierarchically superior to the first digital certificate issuing authority.

2. (Previously Presented) The method of claim 1 wherein signing the electronic document to obtain a once signed electronic document further comprises:

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

3. (Previously Presented) The method of claim 1 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document further comprises:

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

4. (Previously Presented) The method of claim 3 wherein calculating the hash value comprises providing as input to the hash algorithm at least one of:

the party's authenticating information;

the first digital certificate issuing authority's authenticating information;

the digital signature of the first digital certificate issuing authority; or

the second digital certificate issuing authority's authenticating information.

5. (Original) The method of claim 1, wherein writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

6. (Previously Presented) A system comprising:

a bus;

a data storage device coupled to said bus; and

a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing, by the first digital certificate issuing authority, the electronic document to obtain a once signed electronic document;

transmitting the once signed electronic document to a second digital certificate issuing authority;

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party;

wherein the second digital certificate issuing authority is hierarchically superior to the first digital certificate issuing authority.

7. (Previously Presented) A system as in claim 6 wherein signing the electronic document to obtain a once signed electronic document comprises:

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

8. (Previously Presented) A system as in claim 6 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document comprises:

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

9. (Previously Presented) A system as in claim 8 wherein calculating the hash value comprises providing as input to the hash algorithm at least one of:

the party's authenticating information;

the first digital certificate issuing authority's authenticating information;

the digital signature of the first digital certificate issuing authority; or

the second digital certificate issuing authority's authenticating information.

10. (Previously Presented) A system as in claim 6 wherein writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

11. (Previously Presented) An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising:

writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document;

signing, by the first digital certificate issuing authority, the electronic document to obtain a once signed electronic document;

transmitting the once signed electronic document to a second digital certificate issuing authority; and

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party;

wherein the second digital issuing authority is hierarchically superior to the first digital certificate issuing authority.

12. (Previously Presented) An article of manufacture as in claim 11 wherein signing the electronic document to obtain a once signed electronic document further comprises:

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the first digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

13. (Previously Presented) An article of manufacture as in claim 11 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document further comprises:

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

providing, as input to a hash algorithm, the contents of the electronic document;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

14. (Previously Presented) An article of manufacture as in claim 13 wherein calculating the hash value comprises providing as input to the hash algorithm at least one of:

the party's authenticating information;

the first digital certificate issuing authorities authenticating information;

the digital signature of the first digital certificate issuing authority; or

the second digital certificate issuing authority's authenticating information.

15. (Original) An article of manufacture as in claim 11 wherein writing a party's authenticating information and a first digital certificate issuing authorities authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection.

16. (Previously Presented) A method comprising:

receiving, from a first digital certificate issuing authority, a once signed electronic document at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority;

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party.

17. (Previously Presented) The method of claim 16 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document further comprises:

providing, as input to a hash algorithm, the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

18. (Previously Presented) A system comprising:

a bus;

a data storage device coupled to said bus; and

a processor coupled to said data storage device, said processor operable to receive instructions which, when executed by the processor, cause the processor to perform a method comprising:

receiving, from a first digital certificate issuing authority, a once signed electronic document at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority;

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party.

19. (Previously Presented) A system as in claim 18 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document further comprises:

providing, as input to a hash algorithm, the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

20. (Previously Presented) An article of manufacture comprising:

a machine-accessible medium including instructions that, when executed by a machine, causes the machine to perform operations comprising:

receiving, from a first digital certificate issuing authority, a once signed electronic document at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority;

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document;

signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document; and

transmitting, by the second digital certificate issuing authority, the twice signed electronic document to the first digital certificate issuing authority and to the party.

21. (Previously Presented) An article of manufacture as in claim 20 wherein signing, by the second digital certificate issuing authority, the once signed electronic document to form a twice signed electronic document further comprises:

providing, as input to a hash algorithm, the contents of the once signed electronic document and the second digital certificate issuing authority's authenticating information;

calculating, by the hash algorithm, a hash value;

encrypting the hash value using the second digital certificate issuing authority's private key; and

writing the encrypted hash value in the electronic document.

22. (Previously Presented) The method of claim 1 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

23. (Previously Presented) The computer system of claim 6 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

24. (Previously Presented) The article of manufacture of claim 11 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

25. (Previously Presented) The method of claim 16 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

26. (Previously Presented) The computer system of claim 18 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.

27. (Previously Presented) The article of manufacture of claim 20 wherein the second digital certificate issuing authority is a root digital certificate issuing authority.